

Activity Executive Report

This report includes important security information about your current network status.

Start Scan: lun, 27 ott 2008 14:57:48 +0100

Campaign Name: Scansione rapida

Activity Id: 4460



Activity summary

Activity Id:	4460		
User:	ipLegion Administrator admin@emaze.net	Supervisor:	-
Campaign Name:	Scansione rapida	Status:	Completed
Start Scan:	lun, 27 ott 2008 14:57:48 +0100	Duration:	00h:31m:54s
Settings:	Preferenze per la scansione rapida		
Targets:	10.4.10.37/32		

10.4.10.37

Host Summary

Operating System:Linux

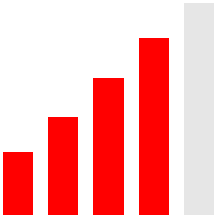
MAC Address:00:0C:29:5F:C0:C0

Hostname:-

Latest activity Exposure Level

HIGH

47



Vulnerability Level

47/100

Bruteforced Accounts

Not Executed

Local Vulnerability Level

Not Executed

Scouts

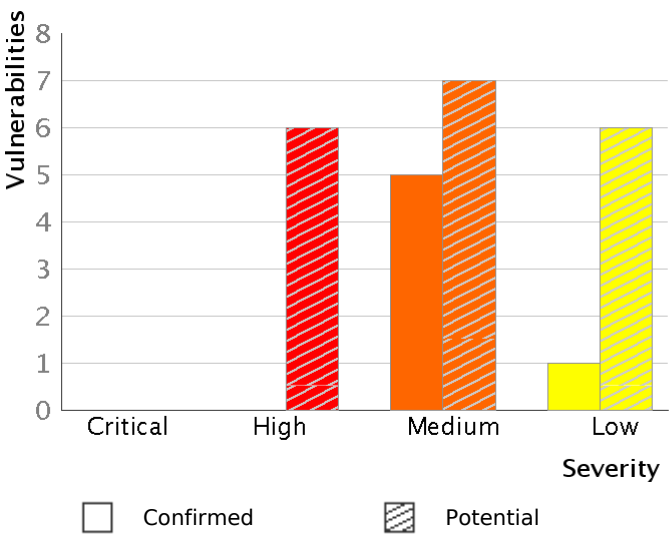
Scout:Scout Rete Test (3)

Vulnerability Assessment Module Results

Vulnerabilities Found

Vulnerabilities Found

Severity	Confirmed	Potential
Critical:	0	0
High:	0	6
Medium:	5	7
Low:	1	6
Total:	6	19



Trend Analysis

No previous scan data available.

Open Ports

Protocol	Port	Service
TCP		
	21	ftp
	22	ssh
	53	domain
	80	tcpwrapped
	111	rpcbind
	139	tcpwrapped
	443	tcpwrapped
	838	rquotad
	1024	status
	1025	sgi_fam
	1026	mountd
UDP		
	53	domain
	111	rpcbind
	137	netbios-ns
	138	netbios-dgm
	835	rquotad
	1024	status
	1026	nlockmgr
	1027	mountd
	2049	nfs

Confirmed Vulnerabilities by Severity

Severity	Vulnerability	Port	Status
Medium	Anonymous FTP Server	21/TCP	New
Medium	SSH Protocol Version 1 Enabled	22/TCP	New
Medium	SSL Certificate Expired	443/TCP	New

Confirmed Vulnerabilities by Severity

Severity	Vulnerability	Port	Status
Medium	SSL Self Signed Certificate	443/TCP	New
Medium	SSLv2 Support Enabled	443/TCP	New
Low	RPC nlockmgr Service allows proxying of NFS requests	1026/UDP	New
Info	DNS Server Running	53/UDP	New
Info	FTP Server Running	21/TCP	New
Info	NFS Server Running	2049/UDP	New
Info	NetBIOS Name Service Running	137/UDP	New
Info	Portmap Daemon Running	111/TCP	New
Info	Portmap Daemon Running	111/UDP	New
Info	RPC nlockmgr Service Running	1026/UDP	New
Info	RPC rquotad Service Running	838/TCP	New
Info	RPC rquotad Service Running	835/UDP	New
Info	RPC status Service Running	1024/TCP	New
Info	RPC status Service Running	1024/UDP	New
Info	Response to ICMP packets	-	New
Info	Response with ICMP Port Unreachable to closed ports	-	New
Info	SSH Server Running	22/TCP	New
Info	SSH Supported Algorithms	22/TCP	New
Info	SSHV2 Key Fingerprint	22/TCP	New
Info	SSL Certificate Information	443/TCP	New
Info	SSL Supported Ciphers List	443/TCP	New
Info	SSL Supported Protocols	443/TCP	New
Info	Software Installed	-	New
Info	UNIX RPC Services	111/TCP	New
Info	UNIX RPC Services	111/UDP	New
Info	VMWare Virtual Machine Running	-	New

The status field is a synthesis of any change that may have occurred between the current and the previous activity of the same campaign. Possible values are: **New**, if the vulnerability wasn't found in the previous activity and was found in the current one. **Already known**, if the vulnerability was found both in the previous and in the current activity. **Removed**, if the vulnerability found in the previous activity wasn't found in the current one. **Port closed**, if the appliance, for some reason, couldn't check in the current activity for a vulnerability that was found in the previous one.

Potential Vulnerabilities by Severity

Severity	Vulnerability	Port	Status
High	OpenSSL Public Key Processing Denial of Service Vulnerability	53/UDP	New
High	OpenSSL ASN.1 Structures Denial of Service Vulnerability	53/UDP	New
High	OpenSSH Buffer Mismanagement Vulnerabilities	22/TCP	New
High	Multiple Vendor libc DNS Resolver Buffer Overflow Vulnerability	53/UDP	New
High	ISC BIND Multiple Remote Denial of Service Vulnerabilities	53/UDP	New
High	ISC BIND 9 Remote Cache Poisoning Vulnerability	53/UDP	New
Medium	OpenSSH LoginGraceTime Remote Denial Of Service Vulnerability	22/TCP	New
Medium	OpenSSH GSSAPI Credential Disclosure Vulnerability	22/TCP	New
Medium	Multiple Vendors BIND 'inet_network()' Off-by-One Buffer Overflow Vulnerability	53/UDP	New
Medium	Multiple DNS Server 'NXDomain' Denial Of Service Vulnerability	53/UDP	New
Medium	ISC BIND TSIG Zone Transfer Denial Of Service Vulnerability	53/UDP	New
Medium	ISC BIND Remote Fetch Context Denial of Service Vulnerability	53/UDP	New
Medium	ISC BIND Remote DNSSEC Validation Denial of Service Vulnerability	53/UDP	New
Low	OpenSSL PKCS Padding RSA Signature Forgery Vulnerability	53/UDP	New
Low	OpenSSH-portable PAM Authentication Remote Information Disclosure Vulnerability	22/TCP	New
Low	OpenSSH-portable Enabled PAM Delay Information Disclosure Vulnerability	22/TCP	New
Low	OpenSSH X connections Session Hijacking Vulnerability	22/TCP	New
Low	OpenSSH Remote Root Authentication Timing Side-Channel Vulnerability	22/TCP	New
Low	OpenSSH PAM Conversation Memory Scrubbing Vulnerability	22/TCP	New

The status field is a synthesis of any change that may have occurred between the current and the previous activity. Possible values are: **New**, if the vulnerability wasn't found in the previous activity and was found in the current one. **Already known**, if the vulnerability was found both in the previous and in the current activity. **Removed**, if the vulnerability found in the previous activity wasn't found in the current one. **Port closed**, if the appliance, for some reason, couldn't check in the current activity for a vulnerability that was found in the previous one.

Legend

Label Description

Exposure Level:	a synthetic benchmark describing the security state of a host. Possible values are: LOW, MEDIUM, HIGH, CRITICAL.
Exposed Host:	a host is exposed when its exposure level is HIGH or CRITICAL.
Confirmed Vulnerabilities:	is detected analysing the host response to such ad hoc request. By consequence, the installed software has a security flaw that may be exploited by an attacker
Potential Vulnerabilities:	is detected analysing the software version contained in the banner of the application response.

Severity Level Description

Vulnerabilities are classified by severity level. There are currently five severity levels: critical, high, medium, low, info.

Critical	A Critical Severity Vulnerability is similar to an High Severity Vulnerability, but it's an especially easy one to exploit. It allows any user with a minimum of technical skill to compromise the affected system. Two kinds of vulnerabilities fall into this category: those that are trivial to exploit (e.g. blank or easy passwords), or those which have an exploit available out of the box in a penetration testing tool (e.g. Metasploit, Core Impact).
High	A High Severity Vulnerability permits a malicious user to directly interfere, at the administrative (root) level, with the structure and functions of the target system via a single vulnerability. Examples of High Severity Vulnerabilities are those which permit a malicious user to access a target system and allows him/her to steal, alter or delete sensitive data stored on it, or to run arbitrary programs.
Medium	A Medium Severity Vulnerability permits a malicious user to externally tamper with the normal operations of a target. Examples of Medium Severity Vulnerabilities are those which let a malicious user mount a Denial of Service (DoS) attack against a target system or access its data.
Low	A Low Severity Vulnerability may help a malicious user to organize an exploit on a target system. However, by itself, it does not constitute a direct breach of the system's security.
Info	These are not technical problems as they are legitimate operations. However, a malicious user can take advantage of these situations to gain useful information which can then be used to form an attack strategy. When deciding whether the service should be kept open or closed, the System Manager will have to judge every case individually.